Enhanced Attack Resilience within Cyber Physical Systems

Rainer Falk, Steffen Fries
Siemens AG
Technology
Munich, Germany
e-mail: {rainer.falk|steffen.fries}@siemens.com

***Abstract*—Cyber physical systems control, monitor, and supervise physical, technical systems using information and communication technology, also called operation technology. The focus of cyber security is protection against cyber attacks, their detection, and recovery from successful cyber attacks. Cyber resilience aims at delivering an intended outcome of the cyber physical system despite attacks and adverse cyber events and even due to failures not directly related to attacks. Industrial security standards define how cyber physical systems and the used devices can be protected against attacks (prevent). Despite all efforts to protect from attacks, it should always be assumed that attacks may happen. Security monitoring allows to detect successful attacks (detect), so that corresponding measures can be performed (react). This paper describes an additional, complementary approach for protecting cyber physical systems. The devices are designed in a way that makes it harder to use them for launching attacks on other devices or on their physical environment. A device-internal hardware-based or isolated firewall limits the network traffic that the device software executed on the device can send or receive. Even if the device software contains a vulnerability allowing an attacker to compromise the device, the technically possible negative impact on other connected devices is limited, thereby enhancing the resilience of the cyber physical system in the presence of manipulated devices.**

Keywords–cyber security; cyber resilience; system integrity; cyber physical systems; industrial automation and control system; Internet of Things.

I. INTRODUCTION

Traditionally, IT security has been focusing on protection of confidentiality, integrity, and availability of data at rest and data in transit, and sometimes also protecting data in use by confidential computing or by applying homomorphic encryption. In cyber physical systems (CPS), major protection goals are availability, meaning that the CPS, e.g., an industrial automation system, stays productive, and system integrity, ensuring that the CPS is in fact operating as intended and designed. Typical industrial application domains are factory automation, process automation, building automation, railway signaling systems, intelligent traffic management, and power system management. Such CPSs are also called *industrial* Internet of Things (IIoT), distinguishing them from other Internet of Things (IoT) domains as, e.g., consumer IoT. Cyber security is covering different phases during operation as there are protect, detect, and react: Protecting against threats, detecting when an attack has occurred, and recovering from successful attacks. With the approach of "resilience under attack", it shall be ensured that the CPS can stay operational even during an ongoing attack, maybe with limited performance or functionality [1]. This property reduces the impact of a successful attack, as the CPS can be continued to be used even if parts of the CPS should have been attacked successfully. The availability of the overall CPS is thereby improved, as the CPS can stay operational even under an ongoing attack.

When designing a security solution for a CPS or for a device used within the CPS, the focus is on protecting the assets of the CPS or device, by preventing attacks against the relevant assets. However, this approach is not complete from a more holistic perspective: It is also important to detect ongoing attacks, and to recover efficiently from an attack. Also, the environment of a device or a CPS has to be protected from attacks originating from a manipulated CPS or one of its devices. In particular, IoT devices have been attacked with the objective to use them for launching attacks against *other* systems. Dao, Phan et al. described distributed denial of service (DDoS) attacks originating from manipulated IoT devices [2]. As (consumer) IoT devices have often also a weak security management, vulnerabilities are often not patched in time, making them an easy attack target. Vulnerable IoT devices connected to the Internet can easily be found by using Internet-based device search engines like Shodan [3] or Morpheus [4].

This paper presents an approach for protecting the network environment, i.e., other devices of a CPS and further connect devices, from attacks originating from a manipulated component of the CPS. It is an extended version of the conference paper [1], extending in particular the possible reduction in risk exposure, see section VI. The objective is to limit the impact of a manipulated CPS device on other devices of the CPS, thereby enhancing resilience of the overall CPS. The intention is to keep the CPS in a trustworthy operational state even if some devices of the CPS should have been successfully attacked and manipulated. The high-level objective addressed by this paper is to present a design for resilient CPS devices that limits the possibility that an attacked device can be used by an attacker for further attacks

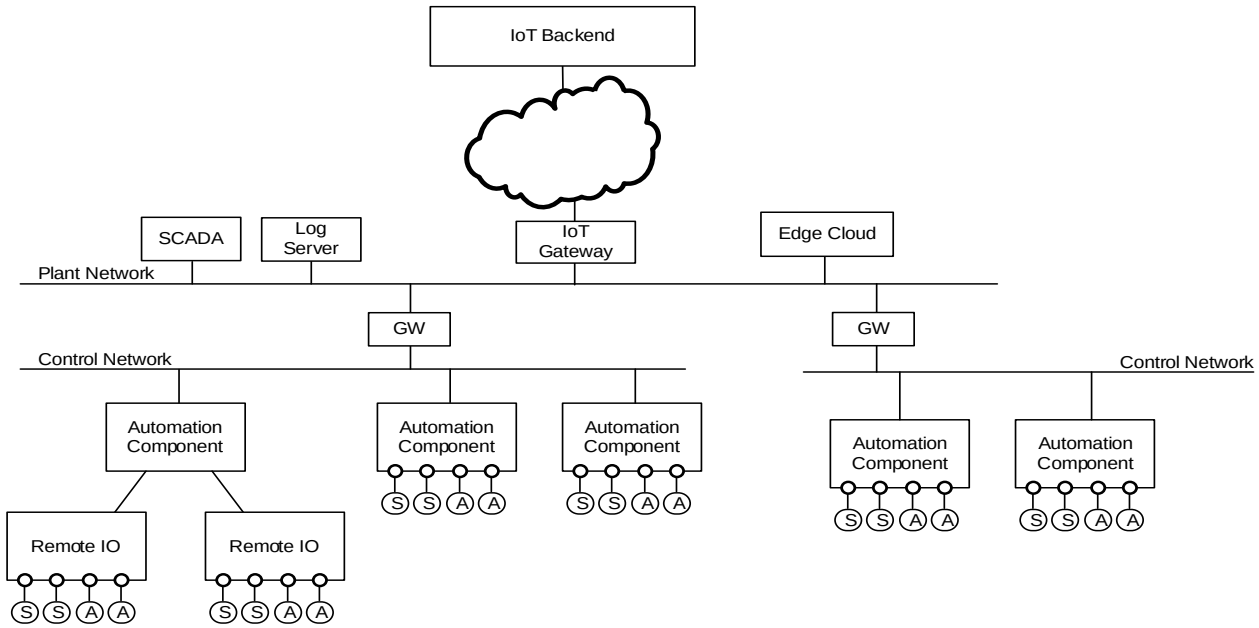

Figure 1. Example – Industrial Automation and Control System

on other devices of the CPS. A manipulated device could otherwise provide manipulated sensor or control data to other CPS devices or manipulate their firmware or configuration data. Such manipulations of CPS devices may finally lead to manipulated control operations impacting the real, physical world, i.e., on the controlled physical process, in a critical way. The main idea is to extend CPS devices with a resilience function that allows to isolate a manipulated operational CPS device from other devices of the CPS. This isolation from other CPS devices extends the isolation from accessing the physical world by a manipulated CPS device by a physical-world firewall [5].

After giving an overview on cyber physical systems and on industrial cyber security and IoT security in Sections II and III, a new approach on protecting the network environment from manipulated devices of a CPS is described in Section V. It is a concept to increase the resilience of a CPS when being under attack. Aspects to evaluate the new approach are discussed in Section VI, investigating the possible reduction of overall risk exposure of the CPS that can be achieved by the presented approach. Section VII concludes the paper.

II. Cyber Physical Systems

A CPS, e.g., an Industrial Automation and Control System (IACS), monitors and controls a technical system. Examples are process automation, machine control, energy automation, and cloud robotics. Automation control equipment with sensors (S) and actuators (A) is connected directly with automation components, or via remote input/output modules. The technical process is controlled by measuring its current state using the sensors, and by determining the corresponding actuator signals. Also, IoT in general can be seen as a cyber physical system, as IoT devices usually interact via the physical world using sensors and actuators [5].

Figure 1 shows an example of an industrial automation and control system, i.e., of an industrial CPS, comprising different control networks connected to a plant network and a cloud backend system. Separation of the network is typically used to realize distinct control networks with strict real-time requirements for the interaction between sensors and actuators of a production cell, or to enforce a specific security policy within a production cell. Such an industrial automation and control system is an example of a CPS and is utilized in various automation domains, including discrete automation (factory automation), process automation, railway automation, energy automation, and building automation.

Figure 2 shows the typical simplified structure of IoT devices, e.g., automation components. The functionality realized by an automation component is largely defined by the firmware/software and the configuration data stored in its flash memory (FW Flash). Such an automation component can also be considered as a remote input/output (IO) device, as in many cases, its operation is controlled by a different control device connected via the network interface (NW IF).

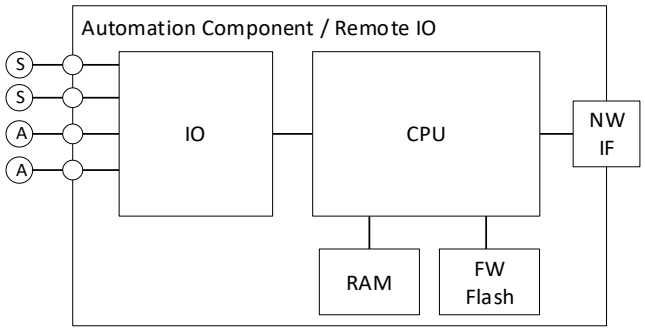

Figure 2. Automation Component

In practice, it has to be assumed that each software component may comprise vulnerabilities, independent of the effort spend to ensure high software quality. This is one reason why automation systems are usually organized in separate security zones. Network traffic can be filtered using network firewalls between different zones, limiting the impact of an impact in one security zone on other connected security zones. In addition, it is often not possible to fix known vulnerabilities immediately by installing a software update, as updates have to be tested thoroughly in a test system before being installed in an operational system, and as an installation is often possible only during a scheduled maintenance window. Also, the priorities of security objectives in different security zones are often different, too. In CPSs, the impact of a vulnerability in an OT system may not only affect data and data processing as in classical IT, but it may have an effect also on the physical world. For example, production equipment could be damaged, or the physical process may operate outside the designed physical boundaries, so that the produced goods may not have the expected quality or even that human health or life is endangered.

III. CYBER SECURITY OF CPS

Protecting IACSs against intentional attacks is increasingly demanded by operators to ensure a reliable operation, and also by regulation. This section gives an overview on industrial security, and on the main relevant industrial security standard IEC 62443 [15]. It summarizes also selected security standards addressing consumer IoT devices.

A. Industrial CPS Security Requirements

Industrial security is called also Operation Technology security (OT security), to distinguish it from general Information Technology (IT) security. Industrial systems have not only different security requirements compared to general IT systems but come also with specific side conditions preventing the direct application of security concepts established in the IT domain in an OT environment. For example, availability and integrity of an automation system often have a higher priority than confidentiality. As an example, high availability requirements, different organization processes (e.g., yearly maintenance windows), and required component or system certifications may prevent the immediate installations of updates.

The three basic security requirements in IT environments are confidentiality, integrity, and availability ("CIA" requirements). This CIA order corresponds to the priority of the basic security requirements typically relevant in common IT systems, However, in automation systems or industrial IT, the priorities are commonly just the other way around: Availability of the IACS has typically the highest priority, followed by integrity. Confidentiality is often no strong requirement for control communications, but may be needed to protect critical business know-how.

Figure 3 shows that in common IT systems, the priority is "CIA". As shown graphically, the CIA pyramid is inverted (turned upside down) in many automation systems.

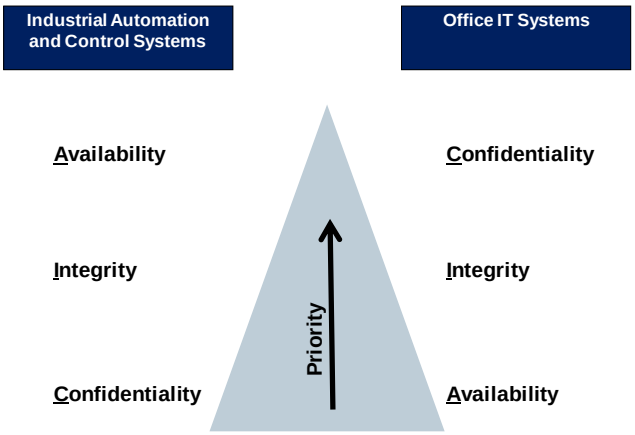

Figure 3. The CIA Pyramid [13]

Specific requirements and side conditions of an IACS like high availability, planned configuration (engineering info), long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing a cyber security solution. Often, an important aspect is that the applied security measures do not put availability and integrity of the automation system at risk. Depending on the considered industry (vertical), they may also be part of the critical infrastructure domain, for which security requirements are also imposed for instance by the European Network and Information Systems (NIS) directive [14] or country specific realizations of the directive. Further security requirements are provided by applying standards defining functional requirements, for instance defined in IEC 62443. The defined security requirements can be mapped to different automation domains, including energy automation, railway automation, building automation, process automation.

Security measures to address these requirements range from security processes, personal and physical security, device security, network security, and application security. No single security technology alone is adequate, but a combination of security measures addressing prevention, detection, and reaction to incidents is required ("defense in depth").

B. Overview IEC 62443 Industrial Security Standard

The international industrial security framework IEC 62443 [15] is a security requirements framework defined by the International Electrotechnical Commission (IEC). It addresses the need to design cybersecurity robustness and resilience into industrial automation and control systems, covering both organizational and technical aspects of security over the life cycle. Specific parts of this framework are applied successfully in different automation domains, including factory and process automation, railway automation, energy automation, and building automation. The standard specifies security for Industrial Automation and Control Systems (IACS) along the lifecycle of industrial systems. Specifically addressed for the industrial domain is the setup of a security organization and the definition of security processes as part of an Information Security

Management System (ISMS) based on already existing standards like ISO 27001 [16] or the NIST cyber security framework. Furthermore, technical security requirements are specified distinguishing different security levels for industrial automation and control systems, and also for the used components. The standard has been created to address the specific requirements of industrial automation and control systems.

Different parts of the IEC62443 standard are grouped into four clusters, covering:

- common definitions and metrics;
- requirements on setup of a security organization (ISMS related, similar to ISO 27001 [16]), as well as solution supplier and service provider processes;
- technical requirements and methodology for security on system-wide level, and
- requirements on the secure development lifecycle of system components, and security requirements to such components at a technical level.

The framework parts address different roles over different phases of the system lifecycle: The operator of an IACS operates the IACS that has been integrated by the system integrator, using components of product suppliers. In the set of corresponding documents, security requirements are defined, which target the solution operator and the integrator but also the product manufacturer.

According to the methodology described in IEC 62443 part 3-2, a complex automation system is structured into zones that are connected by and communicate through so-called "conduits" that connect different zones. A conduit maps, e.g., to the logical network protocol communication between two zones over a firewall. Moreover, this document defines Security Levels (SL) that correspond with the strength of a potential adversary. To achieve a dedicated SL, the defined requirements have to be fulfilled.

Part 3-3 of IEC 62443 [18], addressing an overall automation system, is in particular relevant for the system integrator. It defines seven foundational requirements that group specific requirements of a certain category:

- FR 1 Identification and authentication control
- FR 2 Use control
- FR 3 System integrity
- FR 4 Data confidentiality
- FR 5 Restricted data flow
- FR 6 Timely response to events
- FR 7 Resource availability

For each of the foundational requirements, several concrete technical security requirements (SR) and requirement enhancements (RE) are defined. Related security requirements are defined for the components of an industrial automation and control system in IEC 62443 part 4-2 [19], addressing in particular component manufacturers.

C. Consumer IoT Security

While industrial CPS or industrial automation and control systems are called also industrial IoT, IoT in general includes also consumer IoT. Example consumer IoT devices are connected smoke sensors, connected home automation devices, connected washing machines, or smart cameras.

The standard EN 303 645 [20] defined by the European Telecommunications Standards Institute (ETSI) defines baseline security requirements for consumer IoT devices, addressing cyber security and data protection (user privacy). It is complemented by the assessment specification TS 103 701 [21] and a (draft) implementation guide TR 103 621 [22]. The cyber security provisions defined by EN 303 645 address the following areas:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete user data
- Make installation and maintenance of devices easy
- Validate input data

The defined security requirements or examples also consider resilience of the overall IoT system comprising a huge set of IoT devices, e.g., by randomizing when an update check is performed. Several provisions are defined addressing resilience of the system with respect to outages of data network connectivity or power supply. The main functionality of an IoT device shall be maintained locally when network connectivity is lost, ensuring that the main functionality is available to users independently of network availability. IoT devices may reconnect after power outage with a randomized delay to avoid an overload on the network infrastructure by a huge set of reconnecting IoT devices. This maintains the availability of the network infrastructure after a loss of power in a larger geographic area.

The National Institute of Standards and Technology (NIST) developed a standard for IoT security [23], with an associated catalogue of security requirements [24]. The catalogue defines requirements for the following main cyber security capabilities:

- Device identification
- Device configuration
- Data protection
- Logical access to interfaces
- Software update

– Cybersecurity state awareness
– Device security

In addition, also non-technical, supporting capabilities have been defined:

– Documentation
– Information and query reception
– Information dissemination
– Education and awareness

While resilience in general is not within the addressed scope, the requirements catalogue also includes examples related to resilience, e.g., that an IoT device continues operation when associated networks are unavailable. Furthermore, a draft defining baseline security criteria for consumer IoT devices has been published for comments [25]. A program on trustworthy network of things has been setup, where both IoT devices are protected from the Internet and where the Internet is protected from IoT devices, improving security and robustness of large-scale deployments of IoT devices. One aspect are manufacturer usage descriptions (MUD), as specified in [27], that define the intended communication behavior of an IoT device. It enables a network to block other types of network communication, reducing the attack surface associated to a specific IoT device. It also provides the possibility to automatically configure rules for communication traffic, based on the intended communication behavior. Such rules can be either directly applied, or after inspection and approval by a network administrator.

IV. RESILIENCE UNDER ATTACK

Being resilient means to be able to withstand or recover quickly from difficult conditions [30]. It shifts the focus of "classical" IT/OT cyber security, which puts the focus on preventing, detecting, and reacting to cyber-security attacks, to the aspect to continue to deliver an intended outcome even when an adverse cyber attack is taking place, and to recover quickly back to regular operation [31]. More specifically, resilience of a system is the property to be resistant to a range of threats and withstand the effects of a partial loss of capability, and to recover and resume its provision of service with the minimum reasonable loss of service quality (e.g., performance). It has been addressed in telecommunications, ensuring that subscribers can continue to be served even when one line is out of service [11]. Bodeau and Graubart [32] define resilience guidelines for providers of critical national telecommuni-cations infrastructure in the UK. Kott and Linkov [33] have compiled a book of different contributions addressing various aspects of cyber resilience in networks and systems. Besides an overview on cyber security, metrics to quantify cyber resilience, approaches to assess, analyze and to enhance cyber resilience are described. The notion of resilience is related to risk management, and also to robustness. Risk management, the "classical" approach to cyber security, identifies threats and determines the risk depending on probability and impact of a potential attack. The objective is to put the focus of defined security measures on the most relevant risks. Resilience, however, puts the focus on a reduction of the impact, so that the system stays operational with a degraded performance or functionality even when it has been attacked successfully, and to recover quickly from a successful attack. Robustness is a further related approach that tries to keep the system operational *without* a reduction of the system performance [12], i.e., to withstand attacks.

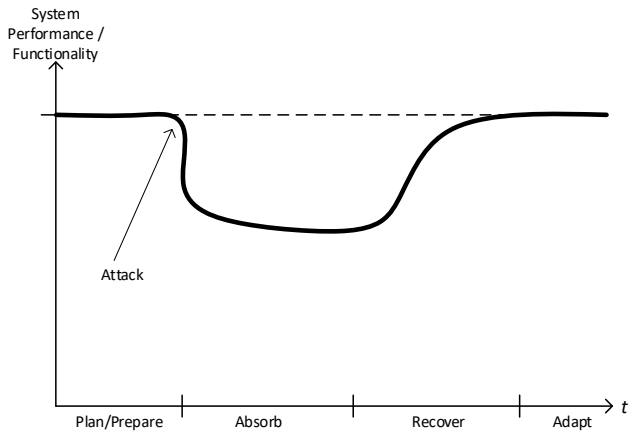

Figure 4. Concept of Cyber Resilience

Figure 4 illustrates the concept of cyber resilience: Even if an attack is carried out, the impact on the system operation, i.e., the performance or functionality of the system, is limited. The effects of an attack are "absorbed", so that the system stays operational, but with limited performance or functionality. A recovery takes place to bring the system up to the regular operation. In adaptation of resilience, the system might be enhanced to better prepare for future attacks. As stated above, a main objective in a CPS is that the CPS stays operational and that its integrity is ensured. In the context of an industrial automation and control system, that means that (only) intended actions of the system in the physical world continue to take place even when the automation and control system of the CPS should be attacked.

The standard NIST SP 800-193 [28] describes technology-independent guidelines for resilience of platform firmware. Resilience-specific roots of trust are defined for update of platform firmware, for detection a corrupted firmware, and for recovery from a compromised platform state. A working group on "cyber resilient technologies" of the Trusted Computing Group (TCG) is working on technologies to enhance cyber resilience of connected systems. Different building blocks for cyber resilient platforms have been described that allow to recover a malfunction device reliably back into a well-defined operational state [29]. Such building blocks enhance resilience as they allow to recover quickly and with reasonable effort from a manipulation. Basic building blocks are a secure execution environment for the resilience engine on a device, protection latches to protect access to persistent storage of the resilience engine even of a compromised device, and watchdog timers to ensure that the resilience engine can in fact perform a recovery. These building blocks are complementary to the extension described in section VI, and they may be used in combination.

V. Protecting Network Environment from Manipulated IoT Devices

The security objective "resilience under attack" means that a CPS, e.g., an IACS or an industrial IoT environment, should stay operational even when some of its components would be manipulated. Considering the manifold of devices used in real-world CPS and practical limitations to timely install patches, it has to be assumed that some of them will have vulnerabilities that can be exploited and be used to also infect further CPS devices. Hence, it shall be avoided that a successfully hacked device can be used to launch attacks against other devices. This is a specific security objective: When designing the security architecture for a device, usually attacks *against* the device are considered. Here, it shall be avoided that a successfully attacked device can be misused by an attacker to launch attacks on other devices within the CPS. So, the possibility to misuse a vulnerable CPS device to launch attacks on other devices of the CPS is reduced.

The software execution environment executes the software (firmware) of the device that might have a vulnerability. A separated, e.g., a separate hardware based, on-device firewall limits the network communication that the executed software can perform. This enforcement is realized independently from the executed device software, so that it is still working even if the device software has been manipulated by an attacker. This independence is a necessary pre-requisite. In the described design, this independence is achieved by separate hardware-based component. However, the independence from the executed device software could be achieved also by using an isolated software execution environment, e.g., a separate processor or a separate trusted execution environment. Using a hardware-based realization has the advantage of limiting the impact on real-time communication properties as delay and jitter, and also on the energy consumption. It can be easily implemented if a dedicated hardware-based network interface is in use anyhow to support real-time communication protocols.

Possible filter criteria are source and destination network addresses, protocols (e.g., TCP, UDP), port numbers, transmit rate (frames/packets per second), or data volume. In an advanced form, the firewall may even verify on application level whether certain control flows are aligned with either the typical (historical) behavior of the device or with the engineered CPS configuration information. The policy might be fixed, e.g., for embedded control devices with a fixed functionality, or it may be configurable. Important is that the device software cannot modify the filter policy on its own.

The filter policy might be adapted automatically depending on the patch status of the device software, or depending on the result of a device integrity self check of the IoT device, or based on a cryptographically protected health check confirmation received from a device integrity monitoring service. This would allow to keep the system operational, although with potentially limited capabilities, thus keeping it resilient. Also, limiting specific functionalities as result of missing device integrity may stipulate the timely application of patches, to get the system back to normal operation with full functionality and performance.

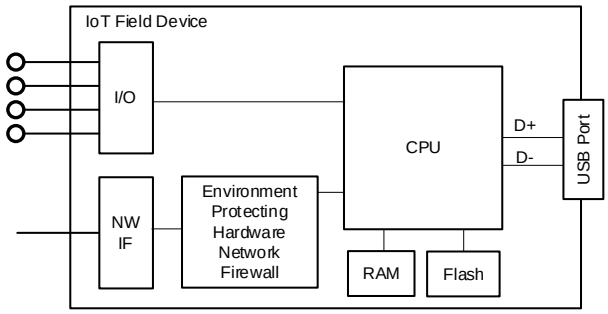

Figure 5. Attack-preventing IoT Device Architecture

Figure 5 shows an IoT Field Device with a central processing unit CPU executing device firmware/software stored in a flash of RAM memory. The software can communicate over the network interface (NW IF) with other devices, e.g., using HTTPS or OPC UA over TCP/IP. Also, sensors and actuators can be connected via an input-output (I/O) interface. An USB interface allows to configure the device or to install a firmware update.

To enhance resilience, the device includes a hardware-based network firewall to protect the network environment from attacks originating from the IoT field device. It limits the type of network communication that can be performed by the device software executed on the CPU. This function is fixed, so that the device software cannot modify it, so that the filtering is performed with high level of trustworthiness. It would be possible as well to use a secure execution environment that is isolated from the main device software executed on its CPU. In both cases, the network firewall is effective even if the main device software executed on the CPU should be manipulated.

The hardware-based firewall can be realized by an integrated circuit, e.g., an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), or a separate microcontroller or security controller, or it can be integrated with a hardware-based network interface. The filter policy might be adapted, depending on whether a cryptographically protected network access token (NAcT) is provided to the hardware firewall. The NAcT can be provided by a backend device integrity check service. The device software may provide a received NAcT token to the device hardware firewall, but cannot manipulate it. This allows the backend device integrity check service to temporarily activate a less restrictive policy if the device integrity has been verified successfully. A NAcT token can be protected by a cryptographic checksum, e.g., a digital signature (e.g., RSA, DSA, ECDSA) or a symmetric message authentication code (e.g., HMAC, AES-CBC-MAC). The NAcT token realizes an authenticated watchdog, as described by England, Aigner, Marochko, Mattoon, Spiger, and Thom [7]. However, here it is used for selecting a firewall policy, not for initiation a device recovery procedure. If an integrity monitoring system monitoring the integrity of control devices or a network-based intrusion detection system, realizing the device integrity check service, detects an ongoing attack in the IACS, it can limit reliably the network communications of devices, allowing to confine the attack.

A different approach compared to attack monitoring is to monitor write access to the flash memory, i.e., to check whether the device software (firmware) stored in the flash memory is updated regularly. The less restrictive, open filter policy stays activated only if the device firmware is updated regularly.

This section described a hardware network firewall of an IoT device to prevent attacks of a manipulated IoT device via network communications. A related, complementary approach, limiting access to the physical world via the sensors and actuators connected to the input/output interface by manipulated software running on the CPU has been described in previous work [6].

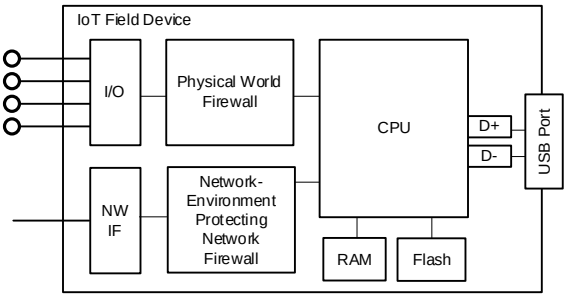

Figure 6. IoT Device Architecture protecting against attacks on both the physical and the cyber environment

Both approaches can be combined in a single IoT device, see Figure 6. The impact of successful attacks on an IoT device on both the network environment as well as on physical world is limited. The possibility that a manipulated IoT device can be used for launching attacks on other connected systems is reduced. While shown as separate entities, both firewall functionalities can also be combined into a single on-device firewall functionality, protecting both access to physical world via I/O interfaces as well as access to other devices by data communication. After having detected a device manipulation by a device integrity check, restrictive filtering policies would be activated in a reliable way by the device so that a manipulated software executed on the CPU has only limited possibilities to perform unwanted sensitive operations impacting the physical world or other IoT devices of the CPS.

VI. EVALUATION

While the original motivation for ”plug and produce”, as defined for Industry 4.0, is to increase flexibility in production and to reduce the time needed to reconfigure an automation environment for different manufacturing tasks or batches, this flexibility is also advantageous for increasing resilience under attack: Even if some of the devices are manipulated (attacked) and cannot be used for production until they are patched, the flexibility of the overall production system allows to reconfigure the IACS components, avoiding or at least limiting the interaction with affected devices. Therefore, production can continue, maybe with limitations, even when some devices should have been manipulated. This means that functionality coming with Industry 4.0 can already be used also to increase resilience under attack, i.e., to improve availability of automation and production systems being under attack. When using the enhancement described in section V, it depends on the specific IACS and on the specific attack scenario to what degree the IACS can stay operational under which specific attack scenario. For the evaluation, it has to be determined to what degree relevant risks of the IACS are reduced by introducing such protection measures.

The security of a CPS is evaluated in practice in various approaches and stages of the system’s lifecycle:

– A Threat and Risk Analysis (TRA, also abbreviated as TARA) is typically conducted at the beginning of the product design or system development, and updated after major design changes, or to address a changed threat landscape. In a TRA, possible attacks (threats) on the system are identified. The impact that would be caused by a successful attack and the probability that the attack happens are evaluated to determine the risk of the identified threats. The risk evaluation allows to prioritize the threats, focusing on the most relevant risks and to define corresponding security measures. Security measures can target to reduce the probability of an attack by preventing it, or by reducing the impact.

– Security checks can be performed during operation or during maintenance windows to determine key performance indicators (e.g., check compliance of device configurations) and to verified that the defined security measures are in fact in place.

– Security testing (penetration testing, also called pentesting for short) can be performed for a system that has been built, but that is currently not in operation. A pentest can usually not be performed on an operational automation and control system, as the pentest could endanger the reliable operation auf the system. Pentesting can be performed during a maintenance window when the physical system is in a safe state, or using a separate test system. Security testing can be performed also on a digital representation of a target system, e.g., a simulation in the easiest case. This digital representation is also called “digital twin”. This allows to perform security checks and pentesting for systems that are not existing yet physically (design phase), or to perform pentesting of operational systems in the digital world without the risk of disturbing the regular operation of the real-world system. Using a dedicated test system or a digital twin simulation environment allows also to install patches and to test their effectiveness and possible influence on the CPS operation without interfering with the operational system.

As long as the technology proposed in the paper has not been proven in a real-world operational setting, it can be evaluated conceptually by analyzing the impact that the additional security measure would have on the identified residual risks as determined by a TRA. The general effect of the presented resilience-under attack security measure is that the worst-case impact of a threat, i.e., a successful attack, on the physical world controlled by the CPS is reduced. Whatever attack is ongoing on the IT-based automation and

control system, still the possible impact on the real, physical world is limited. While security measures often target the prevention of attacks, the proposed resilience measure reduces the impact and thereby the risk. The impact of a threat is reduced if the IACS in fact can stay operational, at least with limited functionality, in relevant attack scenarios. A further, indirect effect of the improved resilience would be that relevant key performance indicators of the CPS, e.g., its uptime/availability, the output of produced goods, the required production time, quality-relevant metrics of produced goods, or the number of deficient goods are maintained even when the CPS is being attacked.

However, TRAs for real-world CPS are not available publicly. Nevertheless, an illustrative example may be given by a chemical production plant performing a specific process like refinery, or a factory producing glue or cement. If the plant is attacked, the attack may target to destroy the production equipment by immediately stopping the process leading to physical hardening of the chemicals / consumables and thus to a permanent unavailability of the production equipment. In this case, trusted sensors could be used to detect a falsified sensor signal, and the physical-world firewall can be used to limit actions in the physical world. Both, the trusted sensors and the physical world firewall build a security overlay network, independent from the actual operational control network. Thereby, a physical damage of the production equipment can be avoided. If needed, a controlled shutdown of the production site can be performed.

Threat	Likelihood	Impact	Risk
Device communication intercepted	unlikely	moderate	minor
Device communication manipulated	unlikely	critical	moderate
Vulnerability in unpatched device exploited	likely	critical	major
Device replaced by fake device	possible	moderate	moderate
⋮	⋮	⋮	⋮

Figure 7. Example Threats of a Threat and Risk Analysis

Figure 7 shows a simplified table as used typically in a threat and risk analysis to collect and evaluate relevant treats to a technical system or component. Some selected threats are shown as examples. Realistic TRAs for real-world systems and components include usually a much longer list of threats. The likelihood and the impact of the threat is determined by judgement of competent personal, usually in a team including technical experts and people responsible for the product or system. The corresponding risk is determined based on likelihood and impact. It has shown to be useful to define and document explicitly the criteria leading to the categorization of likelihood and impact, including also the made assumptions on the operational environment. The TRA with prioritized risks is the basis for security design decisions, focusing on the most critical risks. It is the basis to define a security concept that includes suitable protection measures. Protection measures may not be technical measures only, but include as well organizational and personal security measures (e.g., performing regularly security audits and security trainings).

Figure 8 shows how the likelihood and the impact are mapped to the corresponding risk value. In the example, the three categories unlikely, possible, and likely are used to describe the likelihood. For the impact, the three categories negligible, moderate, and critical are used. In practice, also more fine-granular rankings can be used, distinguishing, e.g., four or five different categories. Also, the risk evaluation can in general include further categories, e.g., disastrous.

For the example threats shown in Figure 7, the risk that the device communication is intercepted is evaluated as minor, as the assumption in the example is that the device communication is protected cryptographically (e.g., by the Transport Layer Security protocol TLS [42]), and that the data would not reveal highly sensitive information.

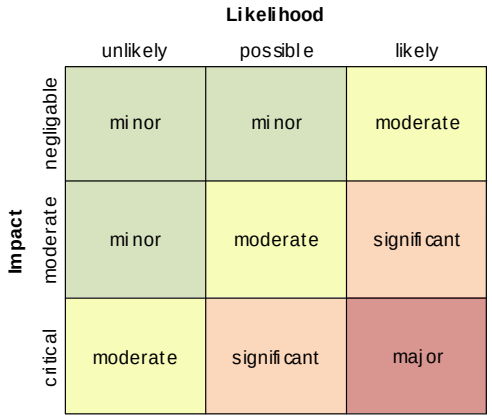

Figure 8. Risk Mapping

The risk that the communication is manipulated, leading to a manipulated device operation, is unlikely as well as the communication is assumed to be protected in transit.

However, the impact is evaluated as critical, as, without any further protection, this threat could lead to arbitrary effects on the device operation and therefore also on the CPS. The risk that a vulnerability of the software running on the device is exploited is ranked here as major, as the assumption is that the device is not regularly patched while being connected to the public Internet. Therefore, it is likely that the vulnerability will be exploited. The functionality of the manipulated device could be changed in arbitrary ways, so that the impact can be critical, leading to a major risk. The threat that the device is replaced by a fake device is evaluated as moderate.

An overview on the determined risks can be shown in a graphical risk reporting as shown in Figure 9. It gives an easily understandable representation on the distribution of identified risks. This representation can be useful to depict the overall risk exposure of a CPS if many risks have been identified. In particular, the example shows one major threat (red field) as well as a moderate threat (yellow field) having a critical impact. Butting resilience measures as the one described in section V into place can reduce the impact of threats, thereby improving the overall risk exposure.

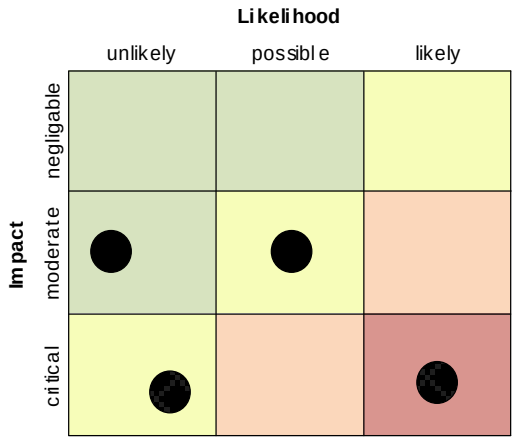

Figure 9. Risk Reporting for the Example Threats without Resilience-Under-Attack Protection

If the resilience under attack protection as described in section IV is put into place, the possible impact of the threats is reduced. This effect is illustrated in Figure 10. As, in the example shown, the impact of the two risks with critical impact reduces from critical to moderate, the risk is reduced correspondingly. Thereby, also the overall risk situation of the overall CPS in which the considered device is used, is improved.

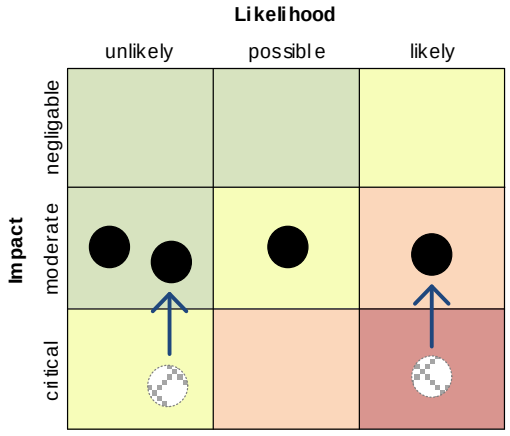

Figure 10. Risk Reporting for the Example Threats with Resilience-Under-Attack Protection

As the evaluation in a real-world CPS requires significant effort, and as attack scenarios cannot be tested that could really have a (severe) impact on the physical world, a simulation-based approach or using specific testbeds are possible approaches, allowing to simulate the effect on the physical world of certain attack scenarios with compromised components in a simulation model of the CPS, or to evaluate it in a protected testbed, e.g., a CPS test system. The simulation would have to include not only the IT-based control function, but also the physical world impact of an attack. Using physical-world simulation and test beds to evaluate the impact of attacks have been described by Urbina, Giraldo et al. [43]. They allow to analyze the impact of successful attacks on the physical world in a safe evaluation environment.

VII. CONCLUSION

A CPS comprises the operational cyber-technology and the physical world with which the system interacts. Both parts have to be covered by a security concept and solution. Traditional cyber security puts the focus on the cyber-part, i.e., automation and control systems. The security of the physical part, like machinery, is protected often by physical and organizational security measures, only. This paper presented a concept for a new approach that enhances the resilience of a CPS in the presence of attacked devices, by making it harder that a compromised CPS device is used for attacking other devices of the CPS. This can be a useful element to ensure the availability of the automation system. Even under attack, the automation system has not to be shut down completely. It can stay operational, possibly with reduced performance or functionality. It is complementary to other approaches for enhancing CPS resilience by protecting the physical-world interface [5] as well as to platform resilience measures as known from [28] [29] that allow to recover a manipulated device quickly and reliably back into a well-defined state.

Possible future work is to not only analyze the effect on reducing the risk exposure of a complex real-world CPS, but to determine the effect of successful attacks on relevant operational key performance indicators of the CPS, as, e.g., uptime and output of a production system. A CPS simulation environment, i.e., a digital twin of the CPS, or a non-operational CPS testbed can be used to analyze the impact of different attack scenarios on CPS key performance indicators that are relevant to the operation of the CPS in a safe way. Such analysis is considered to be relevant in particular for CPS, as attacks may impact not only IT-related assets, but may have also an impact on both the real, physical world of the controlled technical system and on the business-relevant operation of the CPS.

REFERENCES

[1] R. Falk and S. Fries, “Enhancing Attack Resilience in the Presence of Manipulated IoT Devices within a Cyber Physical System”, The Sixth International Conference on Cyber-Technologies and Cyber-Systems CYBER 2021, pp. 1-6, October 03, 2021 to October 07, 2021 - Barcelona, Spain, [Online]. Available from https://www.thinkmind.org/index.php?view=article&articleid=cyber_2021_1_20_80046 [retrieved March, 2023]

[2] N. N. Dao, T. V. Phan, U. Sa’ad, J. Kim, T. Bauschert, and S. Cho, “Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning”, arXiv: 1711.06041v3 [cs.NI] 7 Aug 2019, [Online]. Available from: https://arxiv.org/pdf/1711.06041.pdf [retrieved March, 2023]

[3] Shodan - Search engine for the Internet of everything, [Online], https://www.shodan.io/, [retrieved March, 2023]

[4] Morpheus – Network Security Scanner, [Online], https://www.morpheus.com.na/, [retrieved March, 2023]

[5] R. Falk and S. Fries, “Enhancing Resilience by Protecting the Physical-World Interface of Cyber-Physical Systems”, The Fourth International Conference on Cyber-Technologies and Cyber-Systems CYBER 2019, pp. 6–11, September 22, 2019 to September 26, 2019 - Porto, Portugal, [Online]. Available from: https://www.thinkmind.org/index.php?view=article&articleid=cyber_2019_1_20_80033 [retrieved March, 2023]

[6] R. Falk and S. Fries, “Enhancing the Resilience of Cyber-Physical Systems by Protecting the Physical-World Interface”, International Journal On Advances in Security, volume 13, numbers 1 and 2, pp. 54-65, 2020, [Online]. Available from: http://www.thinkmind.org/index.php?view=article&articleid=sec_v13_n12_2020_5 [retrieved March, 2023]

[7] P. England, R. Aigner, A. Marochko, D. Mattoon, R. Spiger, and S. Thom, “Cyber resilient platforms”, Microsoft Technical Report MSR-TR-2017-40, Sep. 2017, [Online]. Available from: https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/ [retrieved March, 2023]

[8] Electronic Communications Resilience&Response Group, “EC-RRG resilience guidelines for providers of critical national telecommunications infrastructure”, version 0.7, March 2008, available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62281/telecoms-ecrrg-resilience-guidelines.pdf [retrieved March, 2023]

[9] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cardenas, “Attacking fieldbus communications in ICS: applications to the SWaT testbed”, Singapore Cyber-Security Conference (SG-CRC), IOS press, pp. 75–89, 2016, [Online]. Available from: http://ebooks.iospress.nl/volumearticle/42054 [retrieved March, 2023]

[10] C. C. Davidson, T. R. Andel, M. Yampolskiy, J. T. McDonald, W. B. Glisson, and T. Thomas, “On SCADA PLC and fieldbus cyber security”, 13th International Conference on Cyber Warfare and Security, National Defense University, Washington, DC, pp. 140–148, 2018

[11] D. Bodeau and R. Graubart, “Cyber resiliency design principles”, MITRE Technical Report, January 2017, [Online]. Available from: https://www.mitre.org/sites/default/files/publications/PR%20170103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf [retrieved March, 2023]

[12] A. Kott and I. Linkov (Eds.), “Cyber Resilience of Systems and Networks”, Springer, 2019

[13] R. Falk and S. Fries, “Enhancing integrity protection for industrial cyber physical systems”, The Second International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2017, pp. 35–40, November 12 - 16, 2017, Barcelona, Spain, [Online]. Available from: http://www.thinkmind.org/index.php?view=article&articleid=cyber_2017_3_30_80031 [retrieved March, 2023]

[14] European Commission, “The directive on security of network and information systems (NIS Directive)”, [Online]. Available from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [retrieved March, 2023]

[15] IEC 62443, “Industrial automation and control system security” (formerly ISA99), [Online]. Available from: https://webstore.iec.ch/searchform&q=62443 [retrieved March, 2023]

[16] ISO/IEC 27001, “Information technology – security techniques – Information security management systems – requirements”, October 2013, [Online]. Available from: https://www.iso.org/standard/54534.html [retrieved March, 2023]

[17] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”, Version 1.1, April 16, 2018, [Online]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [retrieved March, 2023]

[18] IEC 62443-3-3:2013, “Industrial communication networks – network and system security – Part 3-3: System security requirements and security levels”, Edition 1.0, August 2013

[19] IEC 62443-4.2, “Industrial communication networks - security for industrial automation and control systems - Part 4-2: technical security requirements for IACS components”, February 2019

[20] EN 303 645, “Cyber Security for Consumer Internet of Things: Baseline Requirements”, ETSI, V2.1.1 (2020-06), June 2020, [Online]. Available from: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf [retrieved March, 2023]

[21] TS 103 701, “Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements”, ETSI, V1.1.1 (2021-08), August 2021, [Online]. Available from: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf [retrieved March, 2023]

[22] TR 103 621, ” Guide to Cyber Security for Consumer Internet of Things”, ETSI, Draft 0.0.6 (2021-06), June 2021.

[23] M. Fagan, J. Marron, K. Brady, B. Cuthill, K. Megas, R. Herold, D. Lemire, B. Hoehn, “IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements”, NIST SP 800-213, November 2021, [Online]. Available from: https://csrc.nist.gov/publications/detail/sp/800-213/final [retrieved March, 2023]

[24] M. Fagan, K. Megas, J. Marron, K. Brady, B. Cuthill, R. Herold, D. Lemire, B. Hoehn, “IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog”, NIST SP 800-213A, November 2021, [Online]. Available from: https://csrc.nist.gov/publications/detail/sp/800-213a/final [retrieved March, 2023]

[25] NIST, “DRAFT Baseline Security Criteria for Consumer IoT Devices”, NIST, August 31, 2021, [Online]. Available from: https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf [retrieved March, 2023]

[26] NIST, “Trustworthy Network of Things”, December 15 , 2020, [Online]. Available from: https://www.nist.gov/programs-projects/trustworthy-networks-things [retrieved March, 2023]

[27] E. Lear, R. Droms, D. Romascanu, “Manufacturer Usage Description Specification”, Internet Request for Comments, RFC8520, March, 2019, [Online]. Available from: https://www.rfc-editor.org/rfc/rfc8520.html [retrieved March, 2023]

[28] A. Regenscheid, “Platform Firmware Resiliency Guidelines”, NIST SP 800-193, May, 2018, [Online]. Available from: https://csrc.nist.gov/publications/detail/sp/800-193/final [retrieved March, 2023]

[29] TCG, “Cyber Resilient Module and Building Block Requirements”, V1.0, October 19, 2021, [Online]. Available from: https://trustedcomputinggroup.org/wp-content/uploads/TCG_CyRes_CRMBBReqs_v1_r08_13jan2021.pdf [retrieved March, 2023]

[30] P. England, R. Aigner, A. Marochko, D. Mattoon, R. Spiger, and S. Thom, “Cyber resilient platforms”, Microsoft Technical Report MSR-TR-2017-40, Sep. 2017, [Online]. Available from: https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/ [retrieved March, 2023]

[31] Electronic Communications Resilience&Response Group, “EC-RRG resilience guidelines for providers of critical national telecommunications infrastructure”, version 0.7, March 2008, available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62281/telecoms-ecrrg-resilience-guidelines.pdf [retrieved March, 2023]

[32] D. Bodeau and R. Graubart, “Cyber resiliency design principles”, MITRE Technical Report, January 2017, [Online]. Available from: https://www.mitre.org/sites/default/files/publications/PR%2017-

0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf [retrieved March, 2023]

[33] A. Kott and I. Linkov (Eds.), "Cyber Resilience of Systems and Networks", Springer, 2019

[34] P. Bock, J. P. Hauet, R. Françoise, and R. Foley, "Ukrainian power grids cyberattack - A forensic analysis based on ISA/IEC 62443", ISA InTech magazine, 2017, [Online]. Available from: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack [retrieved March, 2023]

[35] ZVEI, "Orientation guideline for manufacturers on IEC 62443", "Orientierungsleitfaden für Hersteller zur IEC 62443" [German], ZVEI Whitepaper, 2017, [Online]. Available from: https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/ [retrieved March, 2023]

[36] H. R. Ghaeini, M. Chan, R. Bahmani, F. Brasser, L. Garcia, J. Zhou, A. R. Sadeghi, N. O. Tippenhauer, and S. Zonouz, "PAtt: Physics-based Attestation of Control Systems", 22nd International Symposium on Research in Attacks, Intrusions and Defenses, USENIX, pp. 165–180, September 23-25, 2019, [Online]. Available from: https://www.usenix.org/system/files/raid2019-ghaeini.pdf [retrieved March, 2023]

[37] Plattform Industrie 4.0, "Industrie 4.0 Plug-and-produce for adaptable factories: example use case definition, models, and implementation", Plattform Industrie 4.0 working paper, June 2017, [Online]. Available from: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/Juni/Industrie_4.0_Plug_and_produce/Industrie-4.0-_Plug-and-Produce-zvei.pdf [retrieved March, 2023]

[38] T. Hupperich, H. Hosseini, and T. Holz, "Leveraging sensor fingerprinting for mobile device authentication", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, LNCS 9721, Springer, pp. 377–396, 2016, [Online]. Available from: https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2016/09/28/paper.pdf [retrieved March, 2023]

[39] H. Bojinov, D. Boneh, Y. Michalevsky, and G. Nakibly, "Mobile device identification via sensor fingerprinting", arXiv:1408.1416, 2016, [Online]. Available from: https://arxiv.org/abs/1408.1416 [retrieved March, 2023]

[40] P. Hao, "Wireless device authentication techniques using physical-layer device fingerprint", PhD thesis, University of Western Ontario, Electronic Thesis and Dissertation Repository, 3440, 2015, [Online]. Available from: https://ir.lib.uwo.ca/etd/3440 [retrieved March, 2023]

[41] R. Falk and M. Trommer, "Integrated Management of Network and Host Based Security Mechanisms", 3rd Australasian Conference on Information Security and Privacy, ACISP98, pp. 36-47, July 13-15, 1998, LNCS 1438, Springer, 1998

[42] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", Internet RFC8446, August 2018, [Online]. Available from: https://datatracker.ietf.org/doc/html/rfc8446 [retrieved March, 2023]

[43] D. Urbina, J. Giraldo, A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting The Impact of Stealthy Attacks on Industrial Control Systems", ACM Conference on Computer and Communications Security (CCS), pp. 1092–1105, Vienna, Austria, 2016